

## INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

Atty. Docket No.

35.G1868

Application No.

08/777,246

Applicant

KAZUOMI OISHI

Filing Date

DECEMBER 31, 1996

Group

2202

## U.S. PATENT DOCUMENTS

*Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate

RECEIVED  
JAN 28 1998  
GROUP 2200

## FOREIGN PATENT DOCUMENTS

Document Number	Date	Country	Class	Subclass	Translation Yes	No

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Page, Etc.)

H.S.	A	R.L. Rivest, et al. "A Method of Obtaining Digital Signatures and Public-key Cryptosystems", Comm. of ACM 1987, pp. 120-126
	B	H.C. Williams, "A Modification of the RSA Public-Key Encryption Procedure" IEEE Trans. Inf. Theory, IT-26, 6, 1980, pp. 726-729
H.S.	C	A. Shamir, et al. "On the Security of the Merkle-Hellman Cryptographic Scheme", IEEE Trans. Inf. Theory, IT-26, 3, 1980, PP. 339-340
	D	S. Goldwasser, et al. "Strong Signature Schemes", ACM Symp. on Theory of Computing, 1983, pp. 431-439
H.S.	E	S. Goldwasser, et al. "A 'PARADOXICAL' Solution' to the Signature Problem", ACM Symp. on Foundation of Computer Science, 1984, pp.
	F	H. Ong, et al., "An Efficient Signature Scheme Based on Quadratic Equations", ACM Symp. on Theory of Computing, 1984, pp. 208-216

EXAMINER

Ho Song

DATE CONSIDERED

12/22/98

\*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

## INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

Atty. Docket No.

35.G1868

Application No.

08/777,246

Applicant

KAZUOMI OISHI

Filing Date

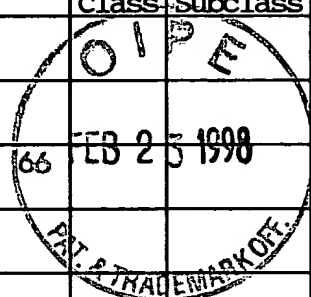
DECEMBER 31, 1996

Group

2202

## U.S. PATENT DOCUMENTS

*Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate



RECEIVED

FEB 24 1998

## FOREIGN PATENT DOCUMENTS

Document Number	Date	Country	Class	Subclass	Translation Yes No

GROUP 2200

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Page, Etc.)

H.S.	A	Ivan Bjerre Damgård, PRACTICAL AND PROVABLY SECURE RELEASE OF A SECRET AND EXCHANGE OF SIGNATURES, Aarhus Univ., Mathematical Inst. pp 200-217
H.S.	B	David Chaum, et al., GROUP SIGNATURES, CWI Centre for Mathematics and Computer Science, Amsterdam, Netherlands, pp. 257-265
H.S.	C	Amos Fiat, et al., HOW TO PROVE YOURSELF: PRACTICAL SOLUTIONS TO IDENTIFICATION AND SIGNATURE PROBLEMS, The Weizmann Inst. Sci. pp 186-194
H.S.	D	Eiji Okamoto, ID-BASED KEY DISTRIBUTION SYSTEM, C&C Information Technology Res. Labs., NEC Corporation, pgs. 15

EXAMINER

H.S. [Signature]

DATE CONSIDERED

12/29/98

\*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO-FB-A820

(also form PTO-1449)

A0000049.DOC (1/24/90)

Patent and Trademark Office-U.S. DEPARTMENT of COMMERCE